PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-242786
(43)Date of publication of application : 08.09.2000

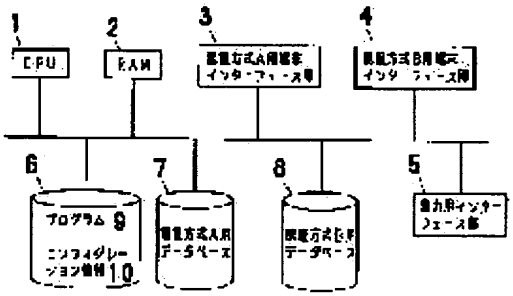
(51)Int.CI. G06T 7/00
// E05B 49/00

(21)Application number : 11-042200
(22)Date of filing : 19.02.1999

(71)Applicant : MATSUSHITA ELECTRIC WORKS LTD
(72)Inventor : YANAGI YASUHIRO
OKADA YUKIO
KOMODA YOSHIYUKI

(54) INDIVIDUAL AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the precison of individual authentication by judging an individual based on the logical product operation value of the theoretical value corresponding to authenticity judgement probability obtained by two or more kinds of authentication systems.
SOLUTION: A CPU 1 receives the information of read features from a terminal for an authentication system A through a terminal interface part 3 for the system A and collates it with features previously stored in a database 7 for the system A so as to perform authentication and judgement based on the system A. Similarly, on the basis of features received from a terminal for an authentication system B, the authentication and judgement are performed based on the system B. The CPU 1 reads out a program 9 stored in a storage device 6, performs final arithmetic processing to the authenticated result of authentication/judgment processing based on the systems A and B with a RAM 2 as a work area and outputs the result to an interface part 5 for output. The information of parameters or the like to be used for arithmetic processing is extracted from configuration information 10, which is stored in the storage device 6, and used for arithmetic processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－242786
（P2000－242786A）
(43)公開日　平成12年９月８日(2000.9.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０	２Ｅ２５０
// Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｒ	５Ｂ０４３
		Ｇ０６Ｆ　15/62	４６５Ｋ	

審査請求　未請求　請求項の数13　ＯＬ　（全９頁）

(21)出願番号　特願平11－42200

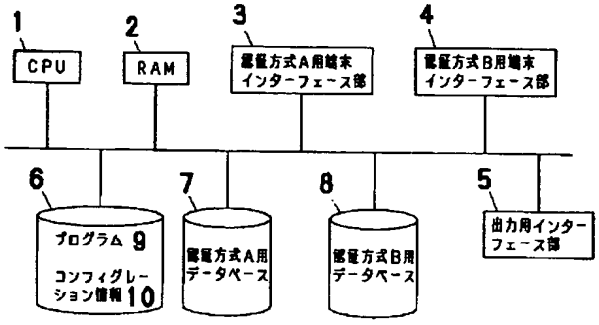
(22)出願日　平成11年２月19日(1999.2.19)

(71)出願人　000005832
松下電工株式会社
大阪府門真市大字門真1048番地
(72)発明者　柳　康裕
大阪府門真市大字門真1048番地松下電工株式会社内
(72)発明者　岡田　幸夫
大阪府門真市大字門真1048番地松下電工株式会社内
(74)代理人　100111556
弁理士　安藤　淳二　（外３名）

最終頁に続く

(54)【発明の名称】　本人認証システム

(57)【要約】
【課題】　本人を認証する精度のさらなる向上が図れる本人認証システムの構造を提供する。
【解決手段】　被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、２種類以上の認証方式を組み合わせ、登録者本人であるかどうかの確率を各認証方式を用いてそれぞれ求め、それぞれの確率が閾値以上かどうかの真偽を判断して各確率に対応する論理値を求め、それらの論理値の論理積演算の値により登録者本人かどうかを判断するように構成した。



1

【特許請求の範囲】

【請求項１】　人間の肉体の特徴を予め登録し、被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、２種類以上の認証方式を組み合わせ、登録者本人であるかどうかの確率を各認証方式を用いてそれぞれ求め、それぞれの確率が閾値以上かどうかの真偽を判断して各確率に対応する論理値を求め、それらの論理値の論理積演算の値により登録者本人かどうかを判断するように構成されていることを特徴とする本人認証システム。

【請求項２】　該当者が複数存在する場合は、確率の値を考慮して、いずれの登録者であるかを判断することを特徴とする請求項１記載の本人認証システム。

【請求項３】　該当者が複数存在する場合は、被験者に特徴の再入力を促し認証処理を再試行することを特徴とする請求項１記載の本人認証システム。

【請求項４】　所定回数再試行を行っても、該当者が複数存在する場合は、確率の値を考慮して、いずれの登録者であるかを判断することを特徴とする請求項３記載の本人認証システム。

【請求項５】　人間の肉体の特徴を予め登録し、被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、２種類以上の認証方式を組み合わせ、登録者本人であるかどうかの確率を各認証方式を用いてそれぞれ求め、それぞれの確率が閾値以上かどうかの真偽を判断して各確率に対応する論理値を求め、それらの論理値の論理和演算の値により登録者本人かどうかを判断するように構成されていることを特徴とする本人認証システム。

【請求項６】　該当者が複数存在する場合は、確率の値を考慮して、いずれの登録者であるかを判断することを特徴とする請求項５記載の本人認証システム。

【請求項７】　２種類以上の認証方式により求められた確率にそれぞれ重み付けを行って閾値以上かどうかの真偽を判断することを特徴とする請求項１または請求項５記載の本人認証システム。

【請求項８】　人間の肉体の特徴を予め登録し、被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、ある認証方式を用いて登録者本人であるかどうかの確率を求め、その確率が閾値を越える候補者を抽出した後、それらの候補者について別の認証方式を用いて登録者本人であるかどうかの確率を求め、閾値以上かどうかを判断して登録者本人かどうかを判断するように構成されたことを特徴とする本人認証システム。

【請求項９】　予め登録した指紋の特徴と、被験者が入力した指紋の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の指の指紋の特徴を登録しておき、認証を行う日時等の条件に応じて、どの指の指紋の特徴を認証に用いるかを変え、入力された指紋の特徴が条件に適合するかを考慮して認証を行うことを特徴とする本人認証システム。

2

【請求項１０】　予め登録した指紋の特徴と、被験者が入力した指紋の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の指の指紋の特徴を登録しておき、予め設定した指の順序に従って指紋の特徴を入力させ認証を行うことを特徴とする本人認証システム。

【請求項１１】　予め登録した顔面の特徴と、被験者が入力した顔面の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の顔面の特徴を登録しておき、認証を行う日時等の条件に応じて、どの特徴を認証に用いるかを変え、入力された顔面の特徴が条件に適合するかを考慮して認証を行うことを特徴とする本人認証システム。

【請求項１２】　予め登録した音声の特徴と、被験者が入力した音声の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の音声の特徴を登録しておき、認証を行う日時等の条件に応じて、どの特徴を認証に用いるかを変え、入力された音声の特徴が条件に適合するかを考慮して認証を行うことを特徴とする本人認証システム。

【請求項１３】　予め登録した筆跡の特徴と、被験者が入力した筆跡の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の筆跡の特徴を登録しておき、認証を行う日時等の条件に応じて、どの特徴を認証に用いるかを変え、入力された筆跡の特徴が条件に適合するかを考慮して認証を行うことを特徴とする本人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、人間の肉体の特徴を登録して本人認証を行うバイオメトリクス技術を用いて、ＢＡ、ＨＡ、その他のセキュリティ分野に応用される本人認証システムに関するものである。

【０００２】

【従来の技術】人間の指紋、顔、音声、筆跡等の情報を利用するバイオメトリクス技術を応用した従来の本人認証システムでは、指紋、顔、音声、筆跡等の各種認証方式のうち、いずれか１つの方式を用い、さらに、指紋認証方式なら右手人差し指、顔面認証方式なら顔の正面、音声認証方式なら「こんにちは」というように、全被験者に同じ条件の情報を要求して判定するように構成されていたため、本人以外を本人として受け入れる（他人受入）が発生し、他人が本人になりすましたり、本人を本人と認識しない（本人拒否）等の確率が高いという精度的な問題点があった。

3

【０００３】
【発明が解決しようとする課題】以上に説明した、本人認証システムの精度的な問題は、本人認証システム自体の性能を向上させることで、ある程度回避することができる。しかし、各認証方式の本人認証システムにおける認証アルゴリズムを改良しても、バイオメトリクス技術を応用した本人認証システムが、生体に関する情報を使用するものである以上、限界があり、本人を認証する性能が頭打ちになることが予想される。
【０００４】本発明は、上記問題点に鑑みなされたもので、その目的とするところは、本人を認証する精度のさらなる向上が図れる本人認証システムの構造を提供することにある。
【０００５】
【課題を解決するための手段】上記目的を達成するため、請求項１記載の本人認証システムは、人間の肉体の特徴を予め登録し、被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、２種類以上の認証方式を組み合わせ、登録者本人であるかどうかの確率を各認証方式を用いてそれぞれ求め、それぞれの確率が閾値以上かどうかの真偽を判断して各確率に対応する論理値を求め、それらの論理値の論理積演算の値により登録者本人かどうかを判断するように構成されていることを特徴とするものである。
【０００６】請求項２記載の本人認証システムは、請求項１記載の本人認証システムで、該当者が複数存在する場合は、確率の値を考慮して、いずれの登録者であるかを判断することを特徴とするものである。
【０００７】請求項３記載の本人認証システムは、請求項１記載の本人認証システムで、該当者が複数存在する場合は、被験者に特徴の再入力を促し認証処理を再試行することを特徴とするものである。
【０００８】請求項４記載の本人認証システムは、請求項３記載の本人認証システムで、所定回数再試行を行っても、該当者が複数存在する場合は、確率の値を考慮して、いずれの登録者であるかを判断することを特徴とするものである。
【０００９】請求項５記載の本人認証システムは、人間の肉体の特徴を予め登録し、被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、２種類以上の認証方式を組み合わせ、登録者本人であるかどうかの確率を各認証方式を用いてそれぞれ求め、それぞれの確率が閾値以上かどうかの真偽を判断して各確率に対応する論理値を求め、それらの論理値の論理和演算の値により登録者本人かどうかを判断するように構成されていることを特徴とするものである。
【００１０】請求項６記載の本人認証システムは、請求項５記載の本人認証システムで、該当者が複数存在する

4

場合は、確率の値を考慮して、いずれの登録者であるかを判断することを特徴とするものである。
【００１１】請求項７記載の本人認証システムは、請求項１または請求項５記載の本人認証システムで、２種類以上の認証方式により求められた確率にそれぞれ重み付けを行って閾値以上かどうかの真偽を判断することを特徴とするものである。
【００１２】請求項８記載の本人認証システムは、人間の肉体の特徴を予め登録し、被験者が入力した特徴を、登録した特徴と照合して認証を行う本人認証システムにおいて、指紋、顔、音声、筆跡等を用いる各種認証方式のうち、ある認証方式を用いて登録者本人であるかどうかの確率を求め、その確率が閾値を越える候補者を抽出した後、それらの候補者について別の認証方式を用いて登録者本人であるかどうかの確率を求め、閾値以上かどうかを判断して登録者本人かどうかを判断するように構成されたことを特徴とするものである。
【００１３】請求項９記載の本人認証システムは、予め登録した指紋の特徴と、被験者が入力した指紋の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の指の指紋の特徴を登録しておき、認証を行う日時等の条件に応じて、どの指の指紋の特徴を認証に用いるかを変え、入力された指紋の特徴が条件に適合するかを考慮して認証を行うことを特徴とするものである。
【００１４】請求項１０記載の本人認証システムは、予め登録した指紋の特徴と、被験者が入力した指紋の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の指の指紋の特徴を登録しておき、予め設定した指の順序に従って指紋の特徴を入力させ認証を行うことを特徴とするものである。
【００１５】請求項１１記載の本人認証システムは、予め登録した顔面の特徴と、被験者が入力した顔面の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の顔面の特徴を登録しておき、認証を行う日時等の条件に応じて、どの特徴を認証に用いるかを変え、入力された顔面の特徴が条件に適合するかを考慮して認証を行うことを特徴とするものである。
【００１６】請求項１２記載の本人認証システムは、予め登録した音声の特徴と、被験者が入力した音声の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の音声の特徴を登録しておき、認証を行う日時等の条件に応じて、どの特徴を認証に用いるかを変え、入力された音声の特徴が条件に適合するかを考慮して認証を行うことを特徴とするものである。
【００１７】請求項１３記載の本人認証システムは、予め登録した筆跡の特徴と、被験者が入力した筆跡の特徴とを照合して認証を行う本人認証システムにおいて、予め各登録者につき、複数の筆跡の特徴を登録しておき、認証を行う日時等の条件に応じて、どの特徴を認証に用

いるかを変え、入力された筆跡の特徴が条件に適合するかを考慮して認証を行うことを特徴とするものである。

【００１８】

【発明の実施の形態】図１に基いて本発明の本人認証システムの一実施形態について説明する。図は、指紋の特徴を用いて認証を行う指紋認証方式、顔面の特徴を用いて認証を行う顔面認証方式、音声の特徴を用いて認証を行う音声認証方式、筆跡の特徴を用いて認証を行う筆跡認証方式等の認証方式のうち、２種類の認証方式Ａ，Ｂを組み合わせたシステムの構成図で、ＣＰＵ１、ＲＡＭ２、認証方式Ａ用端末インターフェース部３、認証方式Ｂ用インターフェース部４、出力用インターフェース部５、記憶装置６、認証方式Ａ用データベース７、認証方式Ｂ用データベース８を備えている。

【００１９】ＣＰＵ１は、記憶装置６に格納されたプログラム９を読み出し、ＲＡＭ２を作業領域として、認証方式Ａによる認証判断処理、及び、認証方式Ｂによる認証判断処理を行った後、それらの認証結果に対し所定の演算処理を行って最終的な認証判断を行うように構成されており、ＣＰＵ１は、その演算処理に用いる変数等の情報を、記憶装置６に格納されたコンフィグレーション情報１０から引き出して演算処理に用いるように構成されている。

【００２０】また、認証方式Ａ用端末インターフェース部３、認証方式Ｂ用端末インターフェース部４には、それぞれ、認証方式Ａに用いる特徴を生体から読み取る認証端末（認証方式Ａ用端末、図示省略）、認証方式Ｂに用いる情報を生体から読み取る認証端末（認証方式Ｂ用端末、図示省略）が接続される。認証方式Ａ用端末と認証方式Ｂ用端末とは、互いに異なる種類の情報を入力する装置であり、それらの端末は、例えば、指紋情報収集用装置、顔面情報収集用カメラ、音声情報収集用マイク、筆跡情報収集用タブレット等である。

【００２１】ＣＰＵ１は、認証方式Ａ用端末インターフェース部３を介して、読み取った特徴の情報を認証方式Ａ用端末から受信し、認証方式Ａ用データベース７に予め格納していた特徴と照合することで認証方式Ａによる認証判断を行うと共に、認証方式Ｂ用端末インターフェース部４を介して、読み取った特徴の情報を認証方式Ｂ用端末から受信し、認証方式Ｂ用データベース８に予め格納していた特徴と照合することで認証方式Ｂによる認証判断を行うように構成されている。但し、認証方式Ａ用端末または認証方式Ｂ用端末の側で認証判断を行い、その結果をＣＰＵ１が受信するように構成してもよい。その場合は、認証方式Ａ用データベース７または認証方式Ａ用データベース８は図示を省略している認証方式Ａ用端末側または認証方式Ｂ用端末側に設けるようにする。

【００２２】次に、ＣＰＵ１は、２つの認証結果に対し所定の演算処理を行って最終的な認証判断を行い、その

結果を出力用インターフェース部５に出力するように構成されている。

【００２３】出力用インターフェース部５は、その最終判断結果に対応した信号を外部の装置に出力する。出力用インターフェース部５が出力する信号は、例えば、ＢＡ，ＨＡ分野では、電気錠の開閉制御に用いられたり、制御監視機能を実現するために用いられ、ＯＡ分野では、サーバーコンピュータへのログインを許可するかどうかの判断処理、コンピュータのスクリーンセーバーを解除するかどうかの判断処理等に用いられる。また、出力用インターフェース部５が出力する信号によって複数の機器を制御するように構成してもよい。

【００２４】次に、記憶装置６に格納されているプログラム９は、認証方式Ａによる認証判断処理を行うプログラムと、認証方式Ｂによる認証判断処理を行うプログラムと、それらの判断処理の結果に基づいて最終判断処理を行うプログラムと、その最終判断結果に応じて処理を実行するプログラム（出力用インターフェース部５への出力処理、アクセスログの記録処理等）等を含んでいる。最終判断処理を行うプログラムは、演算式ｙ＝ｆ（ａ，ｂ，ｍ）の演算を実行する。この演算式で、ｙは認証の最終判断に用いられる値、引数ａは認証方式Ａによる認証判断結果、引数ｂは認証方式Ｂによる認証判断結果、引数ｍはコンフィグレーション情報１０に含まれる、重み付け等の数値である。また、コンフィグレーション情報１０には、認証方式Ａ，Ｂのそれぞれの認証判断に用いる判断基準、または、最終判断処理で用いる演算式、ｍ等の変数が含まれており、これらの情報はユーザー側で修正することができる。

【００２５】認証方式Ａ用データベース７は、認証方式Ａで用いる登録者の生体に関する特徴を登録したデータベースであり、例えば、認証方式Ａを指紋認証方式とすれば、本人である登録者（ユーザー）のＩＤとそのユーザーの指紋の特徴が認証方式Ａ用データベース７に格納されている。同様に、認証方式Ｂ用データベース８にも、認証方式Ｂで用いる、ユーザーの生体に関する情報が格納されている。

【００２６】次に、図２のフローチャートに基いて図に示した本人認証システムの動作について説明する。まず、認証動作が開始されると、認証方式Ａによる認証判断処理、及び、認証方式Ｂによる認証判断処理を行う。具体的には、認証方式Ａ用端末、認証方式Ｂ用端末が読み取った特徴を、それぞれ、認証方式Ａ用端末インターフェース部３、認証方式Ｂ用端末インターフェース部４を介してＣＰＵ１が受信し（認証方式Ａ用端末の出力入手Ｓ１－ａ、認証方式Ｂ用端末の出力入手Ｓ１－ｂ）、それらの情報を、認証方式Ａ用データベース７または認証方式Ｂ用データベース８に予め格納していた特徴と照合することで認証方式Ａ，Ｂによる認証判断を行い（認証方式Ａの判断処理Ｓ２－ａ、認証方式Ｂの判断処理Ｓ

２－ｂ）、それらの判断結果ａ，ｂをＲＡＭ２に一旦出力する（認証方式Ａの判断結果ａ出力Ｓ３－ａ、認証方式Ｂの判断結果ｂ出力Ｓ３－ｂ）。但し、認証方式Ａ用端末または認証方式Ｂ用端末で判断処理を行うように構成した場合はＣＰＵ１は認証方式Ａの判断処理Ｓ２－ａ、認証方式Ｂの判断処理Ｓ２－ｂを行わない。

【００２７】最後に、Ｓ４に示すように、判断結果ａ，ｂ、重み付け変数ｍを用いて演算式ｙ＝ｆ（ａ，ｂ，ｍ）の演算を実行し、Ｓ５に示すように、求めたｙの値に応じて最終判断を行い、その結果を出力する。重み付け変数ｍと演算式ｆ（）はユーザーにより修正が可能である。

【００２８】次に、図１に示した本人認証システムを応用したセキュリティシステムの一実施形態について説明する。図は、建物等への入出退を管理するセキュリティシステムの概略構成を示した図で、本体の入出退セキュリティシステム１１と、指紋認証端末１２と、顔面認証端末１３と、電気錠１４とを備えている。図１に示した本人認証システムは、本体の入出退セキュリティシステム１１の内部に設けられている（図示省略）。図２に示すセキュリティシステムは、予め登録されているユーザーと認証されれば電気錠を開錠状態とし、登録されているユーザーでない場合は入出退セキュリティシステム１１に接続されたネットワーク１５を介して管理室（図示省略）に警報を通知するように構成されている。図３に示すように、このセキュリティシステムに用いられている本人認証システムは、指紋の特徴を用いる認証方式と、顔面の特徴を用いる認証方式とを組み合わせたものである。

【００２９】図３のシステムに用いる本人認証システムは、例えば、ユーザー１００人分の登録情報（ユーザーＩＤ、指紋認証に用いる指紋の特徴に関する情報、及び、顔面認証に用いる顔面の特徴に関する情報）を管理するように構成されており、指紋認証または顔面認証＊で、それぞれ、何点かの特徴点を捉え、記憶装置６に格納している１００人分の登録情報と照合し、登録済みのユーザー１００人のうち、どのユーザーであるかという確率を０～１００％の数値で表現するように構成されている。すなわち、読み取った特徴を、各ユーザーＩＤに対応して格納された特徴点等の情報と照合し、そのユーザーＩＤで表されるユーザーであるかどうかの確率を１００人分について求め配列に格納する。指紋認証判断出力用配列、顔面認証判断出力用配列を、それぞれ、

ａ［］，ｂ［］とすると、指紋認証判断出力用配列ａ［］、顔面認証判断出力用配列ｂ［］は下記のように表される。

指紋認証判断出力用配列ａ［ｐ］＝ｗ

ここで、ｐ：ユーザーＩＤ（１～１００）、ｗ：そのユーザーＩＤのユーザーである確率（０～１００％）

顔面認証判断出力用配列ｂ［ｑ］＝ｘ

ここで、ｑ：ユーザーＩＤ（１～１００）、ｘ：そのユーザーＩＤのユーザーである確率（０～１００％）

次に、指紋認証判断出力用配列ａ［ｐ］及び顔面認証判断出力用配列ｂ［ｑ］に格納された確率（本人確率）に基いて、最終判断を行うための演算処理ｙ＝ｆ（ａ［ｐ］，ｂ［ｐ］，ｍ）を、ｐ＝１～１００について行い、それらの結果に基づいて最終判断を行う。演算式ｆ（）をどのように構成するかによってシステムのセキュリティレベルが異なるが、まず、セキュリティレベルが高いシステムを構成する場合の演算式ｆ（）について説明する。

【００３０】セキュリティレベルが高いシステムとは、すなわち、本人拒否率が上がっても、他人受入率を下げる必要のあるシステムである。指紋認証判断出力用配列ａ［ｐ］及び顔面認証判断出力用配列ｂ［ｑ］の値より、例えば、以下の演算をｒ＝１～１００について行う。

$$y[r]=g(a[r],b[r])*\max(a[r],b[r])$$

・・・（１）式

但し、

ａ［ｒ］≧９０％かつｂ［ｒ］≧９０％の場合

ｇ（ａ［ｒ］，ｂ［ｒ］）＝１

ａ［ｒ］＜９０％またはｂ［ｒ］＜９０％の場合

ｇ（ａ［ｒ］，ｂ［ｒ］）＝０

つまり、関数ｇ（）は、各引数の値（各確率の値）が閾値以上かどうかの真偽を判断して各引数の値に対応する論理値を求め、それらの論理値の論理積演算を行う関数である。また、ｍａｘ（）は、複数の引数のうち、最大の引数の値を求める関数である。

【００３１】例えば、ａ［ｒ１］＝９５％、ｂ［ｒ１］＝９０％の場合、ｇ（ａ［ｒ１］，ｂ［ｒ１］）は１となり、配列ｙ［ｒ１］には、９５％という値が格納される。同様の演算をｒ＝１～１００について行い、その結果、値が０でないｙ［ｒ１］が存在すれば、ユーザーＩＤがｒ１のユーザー本人であると判断するように構成されている。つまり、指紋認証判断による確率及び顔面認証判断による確率が９０％以上であれば、登録されたユーザー本人であると判断するわけである。配列ｙの値が全て０であれば、登録されたユーザーではないと判断し、管理室に警報を通知するように構成されている。

【００３２】また、配列ｙに０でない値が複数存在し、該当者が複数存在する結果になった場合は、配列ｙに格納された値が高い方のユーザーであると判断するようにする。さらに、配列ｙに０でない値が複数存在した場合、情報の再入力から再試行し、その再試行を所定回数繰り返し、それでも、配列ｙに、０でない値が複数存在すれば、配列ｙに格納された値の高い方のユーザーと判

断するように構成してもよい。但し、（１）式は、関数ｇ（）が１の場合、大きい方の確率の値を配列ｙに格納する式であるが、これに限定されず、確率の平均値、確率の最小値等を配列ｙに格納するように構成してもよい。

【００３３】次に、セキュリティレベルが低くてもよい＊

ｙ［ｒ］＝ｈ（ａ［ｒ］，ｂ［ｒ］）＊ｍａｘ（ａ［ｒ］，ｂ［ｒ］）
・・・（２）式

但し、

ａ［ｒ］≧８０％またはｂ［ｒ］≧８０％の場合
ｈ（ａ［ｒ］，ｂ［ｒ］）＝１
ａ［ｒ］＜８０％かつｂ［ｒ］＜８０％の場合
ｈ（ａ［ｒ］，ｂ［ｒ］）＝０

つまり、関数ｈ（）は、各引数の値（各確率の値）が閾値以上かどうかの真偽を判断して各引数の値に対応する論理値を求め、それらの論理値の論理和演算を行う関数である。また、ｍａｘ（）は、複数の引数のうち、最大の引数の値を求める関数である。

【００３４】例えば、ａ［ｒ２］＝８５％、ｂ［ｒ２］＝７０％の場合、ｈ（ａ［ｒ２］，ｂ［ｒ２］）は１となり、配列ｙ［ｒ２］には、８５％という値が格納される。同様の演算をｒ＝１～１００について行い、その結果、値が０でないｙ［ｒ２］が存在すれば、ユーザーＩＤがｒ２のユーザー本人であると判断するように構成されている。つまり、指紋認証判断による確率、顔面認証※

＊システムを構成する場合の演算式ｆ（）について説明する。すなわち、他人受入率が上がっても、本人拒否率を下げる必要のあるシステムである。指紋認証判断出力用配列ａ［ｐ］及び顔面認証判断出力用配列ｂ［ｑ］の値より以下の演算をｒ＝１～１００について行う。

※判断による確率のうち、少なくとも１つが８５％以上であれば、登録されたユーザー本人であると判断するわけである。配列ｙの値が全て０であれば、登録されたユーザーではないと判断し、管理室に警報を通知するように構成されている。

【００３５】また、配列ｙに０でない値が複数存在し、該当者が複数存在する結果になった場合は、配列ｙに格納された値が高い方のユーザーであると判断するようにする。但し、（２）式は、関数ｈ（）が１の場合、大きい方の確率の値を配列ｙに格納する式であるが、これに限定されず、確率の平均値、確率の最小値等を配列ｙに格納するように構成してもよい。

【００３６】さらに、指紋認証方式と顔面認証方式とを組み合わせた本人認証システムで、指紋認証方式に用いる装置の方が精度が高い場合、以下の計算式を実行する。

ｙ［ｒ］＝ｈ（ａ［ｒ］，ｍ＊ｂ［ｒ］）＊ｍａｘ（ａ［ｒ］，ｂ［ｒ］）
・・・（３）式

但し、ｍ＜１．０

つまり、各認証方式の結果を重み付けし、顔面認証方式による確率ｂ［ｒ］より指紋認証方式による確率ａ［ｒ］を重視して最終判断を行うように構成するわけである。また、（３）式は、重み付けを行った後、論理和演算を行う場合の式であるが、重み付けを行った後、論理積演算を行うように構成してもよい。さらに、どの確率にどのような重み付けを行うかはシステムに合わせて最適化すればよい。

【００３７】最後に、指紋認証方式と顔面認証方式とを組み合わせた本人認証システムで、認証処理の速度が重視されるシステムでは、例えば、指紋認証方式による確率ａ［ｒ］をｒ＝１～１００について求め、そのうち、指紋認証方式による確率ａ［ｒ］が９０％以上のユーザー（複数人可）に対してのみ、顔面認証方式による確率ｂ［ｒ］を求め、その確率が９０％以上であった場合にユーザー本人と認めるように構成すればよい。

【００３８】次に、図４に基いて本発明の本人認証システムの異なる実施形態について説明する。但し、図１に示したシステムの構成と同等構成については同符号を付すこととし詳細な説明を省略することとする。図４に示すシステムは、指紋認証方式、顔面認証方式、音声認証方式、筆跡認証方式等の認証方式のうち、いずれか１つの認証方式を用い、登録する情報の種類を複数にして認証のための判断材料を増やすことで、なりすましの防止、他人受入率低減を図るものである。

【００３９】図４に示すシステムは、ＣＰＵ１、ＲＡＭ２、認証端末インターフェース部１６、出力用インターフェース部５、記憶装置６、認証用データベース１７を備えている。ＣＰＵ１は、記憶装置６に格納されたプログラム９を読み出し、ＲＡＭ２を作業領域として、認証端末（図示省略）に入力された情報を記憶装置６に格納しておいた情報と照合して登録された情報であるかを判断し、更に、入力された情報が、登録された情報のうち、予め設定された条件に従った種類のものであるかを判断して本人であるかを最終的に判断するように構成されている。また、判断した結果は、図１に示したシステムと同様に、出力用インターフェース部５を介して外部の機器に出力される。但し、認証端末の側で認証判断を行い、その結果をＣＰＵ１が受信するように構成してもよい。その場合は、認証用データベース１７は、図示を省略している認証端末側に設けるようにする。

【００４０】認証方法についてより具体的に説明すると、指紋情報に基いて認証を行う場合、予め認証用データベース１７に、ユーザー毎に左右あわせて１０指分の指紋情報を登録しておき、例えば、月曜日は右手薬指、

火曜日は左手小指というように、曜日によって異なる指の指紋情報を認証に用いるように構成する。つまり、入力された指紋が認証用データベース１７に登録された指紋であり、かつ、何曜日にどの指の指紋を用いるかという予め設定された条件に適合しているかを判断して認証を行う方式である。何曜日にどの指の指紋を用いるかという条件は、コンフィグレーション情報１０の１つとして記憶装置６に格納しておき、全ユーザーが同じ条件に従うように構成してもよいし、ユーザー毎に異なるように構成してもよい。例えば、火曜日は左手小指の指紋を用いるようにした場合、火曜日に入力された指紋が認証用データベース１７に登録された指紋であっても、その指紋が左手小指の指紋でなければ他人であると判断されるので、他人によるなりすましが発生する確率を低減することができる。

【００４１】同様に、顔面情報を用いて認証を行う場合は、認証用データベース１７に、例えば、ユーザー毎に、正面、右横、左横の３種類の顔面情報を登録しておき、例えば、今週は右横の顔面情報、来週は正面の顔面情報というように、認証を行う週に対応して、異なる顔面情報を用いるように設定しておく。どの週にどの顔面情報を用いるかという条件をコンフィグレーション情報１０の１つとして記憶装置６に格納しておく。このように構成することにより、顔面情報を入力した週は正面の顔面情報を用いるように設定されているのに、入力された顔面情報が右横の顔面情報であれば本人と認証されないので他人によるなりすましが発生する確率を低減することができる。また、顔面情報の種類は、正面、右横、左横等の顔の向きを変えたものに限定されず、顔面情報収集用カメラと顔面との距離を変えた複数種類の顔面情報を用いてもよい。

【００４２】また、音声情報を用いて認証を行う場合、認証用データベース１７に、例えば、ユーザー毎に３種類の音声情報（言葉ａを発音した場合の音声Ａ、言葉ｂを発音した場合の音声Ｂ、言葉ｃを発音した場合の音声Ｃ）を登録しておき、予めコンフィグレーション情報１０の１つとして設定した条件（今週は音声Ａ、来週は音声Ｂ等）に従って、入力された音声が予め設定された種類の音声であるかを判断して認証を行えばよい。

【００４３】筆跡情報を認証に用いる場合は、認証用データベース１７に、ユーザー毎に３種類の筆跡情報（単語Ａを筆記した場合の筆跡情報、単語Ｂを筆記した場合の筆跡情報、単語Ｃを筆記した場合の筆跡情報）を登録しておき、例えば、今週は単語Ａ、来週は単語Ｂというように、週毎に筆記する単語を対応させておき、筆跡が入力された週情報も認証に用いるように構成すればよい。どの週にどの単語の筆跡を認証に用いるかはコンフィグレーション情報１０の１つとして設定しておく。

【００４４】さらに、指紋を認証に用いる場合で、例えば、最初に右手中指の指紋を用いて認証した後、左手親指の指紋を用いて認証して本人と判断するように構成してもよい。認証に用いる指の順序は、コンフィグレーション情報１７の１つとして登録しておき、ユーザー本人しか知らない情報としておく。

【００４５】図５のフローチャートに基いて図４に示した本人認証システムの動作について説明する。まず、認証動作が開始されると、ＣＰＵ１は、認証端末から出力される特徴点等の情報を入手し（Ｓ１）、認証用データベース１７に登録された情報と照合して認証判断処理を行う（Ｓ２）。具体的には、読み取った情報が、認証用データベース１７に登録された情報であるかを判断して登録されたユーザー本人であるかどうかを判断する（Ｓ３）。その結果、読み取った情報が認証用データベース１７に登録されていれば（登録されたユーザー本人の情報であれば）、Ｓ４に示すように読み取った情報（入力情報）の適合性（指紋認証ならどの指の指紋であるか、筆跡認証なら設定した文字であるかどうか等の、予め設定された条件に適合するか）を判断して、適合していれば、登録されたユーザー本人であると最終的に判断する（Ｓ５）。読み取った情報が登録されていない場合、または、読み取った情報が予め設定された条件に不適合と判断された場合は、他人であると判断する。

【００４６】なお、図１に示した本人認証システムで、閾値、組み合わせる認証方式の種類及び数は実施形態に限定されるものではない。

【００４７】

【発明の効果】本願発明の本人認証システムによれば、他人受入率、本人拒否率を低減することで本人認証システムの精度が向上し、より高いセキュリティレベルが要求される用途に対応することができる。また、本人認証システムを組み込むシステムに応じて認証判断時の演算方法をカスタマイズすることで認証レベルを最適化することができる。

【図面の簡単な説明】

【図１】本発明の本人認証システムの一実施形態を示す構成図である。

【図２】図１の本人認証システムの動作を説明するためのフローチャートである。

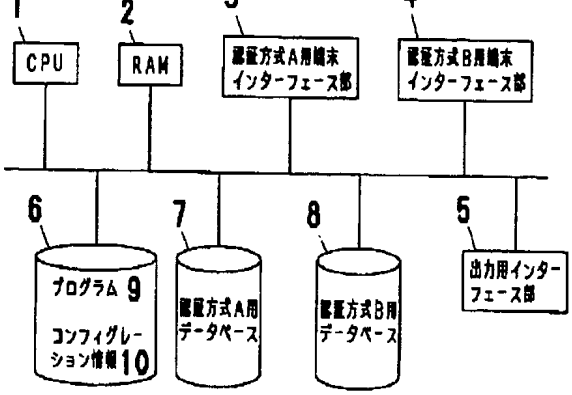
【図３】本発明の本人認証システムを応用した入出退セキュリティシステムの概略構成図である。

【図４】本発明の本人認証システムの異なる実施形態を示す構成図である。

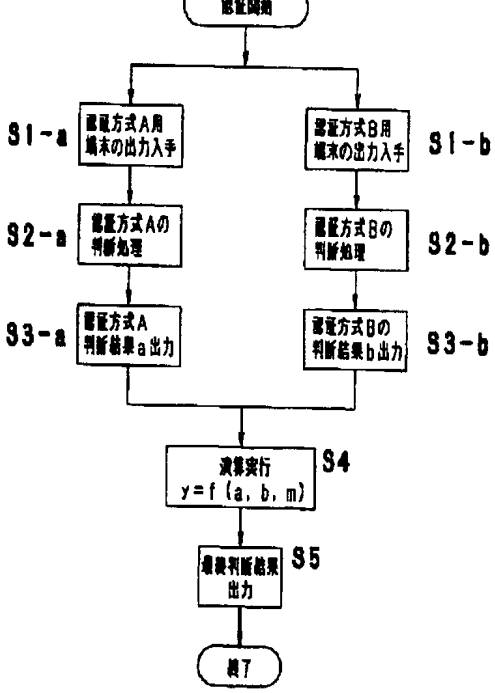
【図５】図４の本人認証システムの動作を説明するためのフローチャートである。

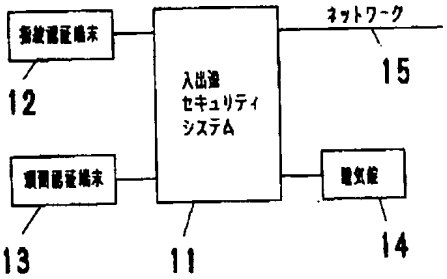
【符号の説明】

１	ＣＰＵ
２	ＲＡＭ
３	認証方式Ａ用端末インターフェース部
４	認証方式Ｂ用インターフェース部
５	出力用インターフェース部

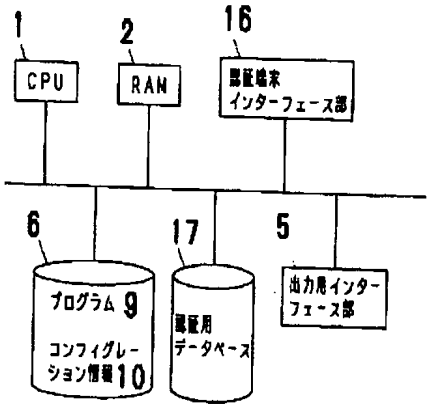

1
CPU
2
RAM
3
認証方式A用端末
インターフェース部
4
認証方式B用端末
インターフェース部
6
プログラム 9
コンフィグレーション情報 10
7
認証方式A用
データベース
8
認証方式B用
データベース
5
出力用インターフェース部

【図3】

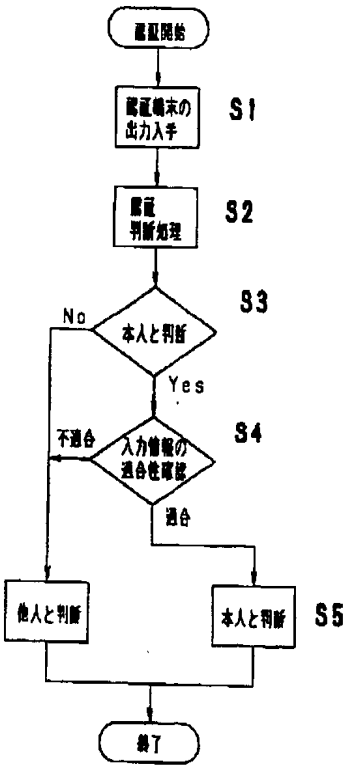

認証開始
S1-a
認証方式A用端末の出力入手
S1-b
認証方式B用端末の出力入手
S2-a
認証方式Aの判断処理
S2-b
認証方式Bの判断処理
S3-a
認証方式A判断結果a出力
S3-b
認証方式Bの判断結果b出力
演算実行
y=f(a, b, m)
S4
最終判断結果出力
S5
終了


指紋認証端末
12
顔面認証端末
13
入出退セキュリティシステム
11
ネットワーク
15
電気錠
14

【図4】


1
CPU
2
RAM
16
認証端末インターフェース部
6
プログラム 9
コンフィグレーション情報 10
17
認証用データベース
5
出力用インターフェース部

【図5】


認証開始
認証端末の出力入手
S1
認証判断処理
S2
No
本人と判断
S3
Yes
不適合
入力情報の適合性確認
S4
適合
他人と判断
本人と判断
S5
終了

フロントページの続き

(72)発明者 薦田 美行
大阪府門真市大字門真1048番地松下電工株式会社内

Ｆターム(参考) 2E250 DD08 DD09 DD10
5B043 AA04 AA09 BA01 BA02 BA06 BA07 CA03 GA13 GA17

THIS PAGE BLANK (USPTO)